REMARKS

1. Status of the Claims

Claims 1-20, 23-25, and 28-30 are pending in the application. Claims 1-4 and 23-25 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over United States Patent No. 5,416,841 ("Merrick") in view of United States Patent No. 6,457,126 ("Nakamura"). Claims 5-8 stand rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and further in view of United States Patent No. 6,823,069 ("Kitajima"). Claim 9 stands rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and further in view of Kitajima and Publication No. US2004/0015953 A1 ("Vincent"). Claim 10 stands rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and further in view of Kitajima and United States Patent No. 6,853,729 ("Mizikovsky"). Claims 11-14 and 28-30 stand rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and United States Patent No. 5,150,407 ("Chan"). Claims 15-18 rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and Chan and further in view of Kitajima. Claim 19 stands rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and Chan and further in view of Vincent. Claim 20 stands rejected under 35 U.S.C.§ 103(a) as unpatentable over Merrick in view of Nakamura and Chan and further in view of Mizikovsky. Applicants respectfully traverse the pending claim rejections for at least the following reasons.

2. Claims 1-10 And 23-25 Are Patentable Over The Cited References

Claim 1 as previously presented recites:

> A method for enabling encryption and decryption of an initial version of a software product comprising the steps of:
>
> generating a first encryption key;

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;

splitting said first encryption key into first and second key portions by (i) generating a first key portion of said first encryption key and (ii) calculating a second key portion of said first encryption key by utilizing said first key portion and said first encryption key to generate said second key portion such that the combination of said first key portion and second key portion form said first encryption key;

providing said first key portion and said second key portion and said encrypted initial software product for use in a hardware product, wherein said first key portion is generated independent of information identifying said hardware product;

combining said first key portion and said second key portion to provide said first encryption key in said hardware product; and

utilizing said first encryption key to decrypt said encrypted initial software product in said hardware product.

Claims 2-10 and 23-25 each depend from claim 1 and, therefore, include the foregoing limitations.

The examiner has rejected claim 1 on the basis that Merrick purportedly teaches, among others, the step of "splitting said first encryption key into first and second key portions (col. 2 lines 47) by (i) generating a first key portion of said first encryption key (fig. 1 element 30 and col. 5 lines 6; short key/first key/n bits); and (ii) calculating a second key portion by utilizing said first key portion and said first encryption key to generate said second key portion of said first encryption key such that the combination of said first key portion and said second key portion form said first encryption key (col. 5 lines 6-11). Office Action at 2-3. Applicants respectfully traverse this basis for rejection.

Applicants submit that Merrick does not teach the step of "calculating a second key portion by utilizing said first key portion and said first encryption key to generate said second

key portion of said first encryption key" either at the passage cited by the examiner or elsewhere. Instead, Merrick unequivocally teaches away from such a limitation. *See* Merrick at col. 3, ll. 45-49 ("[n]ote that ***it is important that the second key is not generated based on the first key***, since this would potentially allow an adversary who had access to either of the first or second keys to determine the other and thereby the full length key") (emphasis added).

Further, Applicants submit that, notwithstanding the language at col. 2, line 47, Merrick does not teach splitting an encryption key into first and second key portions in the first instance. To the contrary, as is clear from the discussion at col. 5, lines 5-11, Merrick teaches generating a key of N-n bits in a key management facility and combining it with a user-generated key of n bits to yield an encryption key of N bits that can be used to encrypt data. Moreover, Merrick does not teach how the user-supplied key portion and the key portion generated by the key management facility are combined. Thus, the concepts of Merrick cannot be used to split the encryption key, once formed, into the first and second key portions.

In view of the above, Applicant's claim 1 cannot be unpatentable over Merrick alone or in view of any other reference. Because claims 2-10 and 23-25 include all of the limitations of claim 1, they, too, cannot be unpatentable over Merrick whether taken alone or in combination with any other reference. Accordingly, Applicants respectfully request reconsideration and withdrawal of the pending rejections of claims 1-10 and 23-25 and timely allowance of these claims.

3. <u>Claims 11-20 And 28-30 Are Patentable Over The Cited References</u>

Claim 11 as previously presented recites:

> A method for providing for the security of encryption keys for encryption and decryption of an initial version of a software product provided to a user of a hardware product, said method comprising:

providing a first encryption key;

encrypting the initial version of the software product with said first encryption key to generate an encrypted initial software product;

splitting said first encryption key into first and second key portions by (i) generating a first key portion of said first encryption key independent of information identifying said hardware product and (ii) utilizing said first key portion and said first encryption key to calculate a second key portion of said first encryption key such that the combination of said first and second key portions form said first encryption key;

storing said first key portion in storage means external to the hardware product;

storing said second key portion separately from said first key portion in a tamper proof memory means in the hardware product;

storing said encrypted software product in a further memory means in the hardware product;

combining said first key portion and said second key portion in the hardware product to provide said first encryption key; and

decrypting said encrypted initial software product with said first encryption key.

Claims 12-20 and 28-30 each depend from claim 1 and, therefore, include the foregoing limitations.

The examiner has rejected claim 11 on the basis that Merrick purportedly teaches, among others, the step of "splitting said first encryption key into first and second key portions (col. 2 lines 47) by (i) generating a first key portion of said first encryption key(fig. 1 element 30 and col. 5 lines 6; short key/first key/n bits); and (ii) utilizing said first key portion and said first encryption key to calculate a second key portion of said first encryption key such that the combination of said first and second key portions form said first encryption key (col. 5 lines 6-11)." Office Action at 10-11.[1] Applicants respectfully traverse this basis for rejection on the

[1] The Office Action indicates at p. 10 that the examiner has applied Nakamura as the primary reference in her rejection of claim 11. The context of this rejection, however, makes clear that

ground that Merrick does not teach "utilizing said first key portion and said first encryption key to calculate a second key portion of said first encryption key" either at the passage cited by the examiner or elsewhere. Instead, Merrick unequivocally teaches away from such a limitation. *See* Merrick at col. 3, ll. 45-49 ("[n]ote that ***it is important that the second key is not generated based on the first key***, since this would potentially allow an adversary who had access to either of the first or second keys to determine the other and thereby the full length key") (emphasis added).

Further, Applicants submit that, notwithstanding the language at col. 2, line 47, Merrick does not teach splitting an encryption key into first and second key portions in the first instance. To the contrary, as is clear from the discussion at col. 5, lines 5-11, Merrick teaches generating a key of N-n bits in a key management facility and combining it with a user-generated key of n bits to yield an encryption key of N bits that can be used to encrypt data. Moreover, Merrick does not teach how it combines the user-supplied key portion and the key portion generated by the key management facility. Thus, the concepts of Merrick cannot be used to split the encryption key, once formed, into the first and second key portions.

In view of the above, Applicant's claim 11 cannot be unpatentable over Merrick, either alone or in view of any other reference. Because claims 12-20 and 28-30 include all of the limitations of claim 11, they, too, cannot be unpatentable over Merrick whether taken alone or in combination with any other reference. Accordingly, Applicants respectfully request reconsideration and withdrawal of the pending rejections of claims 11-20 and 28-30 and timely allowance of these claims.

---

the examiner actually has applied Merrick as the primary reference in her rejection of claim 11 and that she has applied Nakamura and Chan as secondary and tertiary references, respectively.

4. **Applicants' Record of April 16, 2007 Interview**

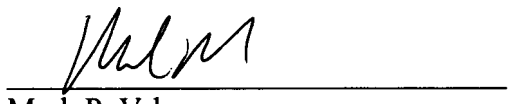
In the previous Office Action bearing mail date February 1, 2007, the examiner rejected claims 1-20 and objected to claims 21-30 as being dependent on rejected base claims but indicated that claims 21-30 would be allowable if rewritten in independent form, including all of the limitations of their respective base claims and any intervening claims. Applicants responded to the February 1, 2007 Office Action on February 23, 2007 by amending the claims to place them into condition for allowance further to the examiner's foregoing indication of allowability.

During a telephonic interview conducted on April 16, 2007, the examiner expressed her intent to withdraw the indication of allowability of claims 21-30 set forth in the February 1, 2007 Office Action and suggested that Applicants add to these claims one or more further limitations directed to the nature of hardware product identifying information that Applicants claimed invention does not use in the generation of first key portion referred to in those claims. For example, the examiner suggested that Applicants amend the claims to recite the hardware product's serial number as an example of such hardware product identifying information. Applicants' attorney responded that the specification does not limit the type of hardware product identifying information not used by the claimed invention and, therefore, that such amendment was unnecessary. The examiner and her supervisor then indicated that the examiner would conduct a further search and issue a further Office Action.

5. Conclusion

Applicants respectfully submit that the application is in condition for allowance and respectfully request reconsideration toward that end.

Respectfully submitted,



Mark P. Vrla
Registration No. 43,973

Dated: July 11, 2007

JENNER & BLOCK LLP
330 North Wabash Avenue
Chicago, IL 60611
Telephone No: (312) 222-9350
Facsimile No: (312) 527-0484